VIRDI 3000 TM User's Manual

Version eng-1.00

UNION COMMUNITY

Copyright 2006 By Union Community Co., Ltd.

Disclaimers

Information in this document is provided in connection with UNION COMMUNITY products. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document. Except as provided in UNION COMMUNITY's Terms and Conditions of Sale for such products, UNION COMMUNITY assumes no liability whatsoever, and UNION COMMUNITY disclaims any express or implied warranty, relating to sale and/or use of UNION COMMUNITY products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right.

UNION COMMUNITY products are not intended for use in medical, life saving, life sustaining applications, or other applications in which the failure of the UNION COMMUNITY product could create a situation where personal injury or death may occur. Should Buyer purchase or use UNION COMMUNITY products for any such unintended or unauthorized application, Buyer shall indemnify and hold UNION COMMUNITY and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that UNION COMMUNITY was negligent regarding the design or manufacture of the part.

UNION COMMUNITY reserves the right to make changes to specifications and product descriptions at any time without notice to improve reliability, function, or design. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." UNION COMMUNITY reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

Please contact UNION COMMUNITY, local UNION COMMUNITY sales representatives or local distributors to obtain the latest specifications and before placing your product order.

About UNION COMMUNITY

With regard to any fingerprint-related issues, UNION COMMUNITY is always in readiness to find out well fitted solutions, depending on customers' requirements and needs.

As a leading provider of fingerprint core technology, UNION COMMUNITY has set up wide variety of fingerprint product lines from fingerprint OEM modules to several choices of fingerprint finished products including access control, time & attendance, door lock, PC peripherals, safety box, etc, that incorporate UNION COMMUNITY's groundbreaking biometrics technology. Based on its proprietary algorithm, its own

sensor and in-house one-stop processing capability regarding hardware, software, product design, etc., our services to government sector and various commercial sectors like security, construction and enterprise are in full swing through fast problem-solving approach to meet market trends or demands. As a result, UNION COMMUNITY exports its market-proven fingerprint products to over 40 countries including Japan, USA, Europe and China.

As the biggest and the most promising company in the commercial sector of biometrics industry in Korea, UNION COMMUNITY was awarded "Korean World-class Product Award" for its excellent performance by Minister of Commerce, Industry and Energy in December 2005.

To be the world-class company in biometrics field, UNION COMMUNITY and all the members continue to do all-out efforts for the world-best quality product, creation of new paradigm and customers' satisfaction through accumulated expertise and working experience from various reference sites and versatile hardware & software development.

About This Manual

This is an introduction to operation of VIRDI 3000 series supplied by UNION COMMUNITY. This manual describes how to do user registration in local terminal, terminal settings, network settings, etc. The purpose of this manual is to provide instructions on using VIRDI 3000 series and troubleshooting minor problems.

< Glossary>

- Admin, Administrator
  - As a user who can enter into the terminal menu mode, he can register/modify/delete terminal users and change the operating environment by changing settings.
  - If there is no administrator for a terminal, anyone can change the settings. In this regard, it is recommended to register at least one administrator.
  - Caution is required with registration and operation because an administrator has the right to change critical environmental settings of the terminal.

- 1 to 1 Verification
  - A user's verification fingerprint (template) is compared to the user's enrollment fingerprint (template) previously registered. The terminal performs 1:1 matches against the user's enrolled template until a match is found.
  - It is called 1 to 1 Verification because only the fingerprint registered in the user's ID or card is used for comparison.

- 1 to N Identification
  - The terminal performs matches against multiple fingerprints (templates) based solely on fingerprint information.
  - Without the user's ID or card, the user's fingerprint is compared to fingerprints previously registered.

- I-Capture (Intelligent Capture)
  - Reinforces detection capability for residual fingerprints (fingerprints left on a sensor window due to sweat or contaminants on a finger) and automatically adjusts sensor settings to detect good-quality fingerprints regardless of the conditions (dry or wet) of the fingerprints.

- Authentication level
  - Depending on the fingerprint match rate, it is displayed from 1 to 9. Authentication is successful only if the match rate is higher than the set level.
  - The higher the Authentication level, the higher the security. However, it requires a relatively high match rate, so Authentication is vulnerable to failure.
  - 1:1 Level: Authentication level used for 1:1 verification
  - 1:N Level: Authentication level used for 1:N identification

- Authentication Method
  - Various kinds of authentication including FP (fingerprint) authentication, PW (password) authentication, RF (card) authentication, or a combination of these methods
  - Ex) FP|PW: fingerprint or password authentication; password is used for authentication if fingerprint authentication fails

- Function keys
  - [F1], [F2], [F3], [F4], [ENTER] are used, and they are used for direct authentication and each key represents each authentication mode.

Table of Contents

< Glossary> **4**
Table of Contents **6**
1. Before use **8**
1.1. Safety precautions **8**
1.2. Terminal description **9**
1.3. Button description **9**
1.4. Operation screen description **10**
1.5. Voice information during operation **11**
1.6. Buzzer sound during operation **11**
1.7. LED signal during operation **11**
1.8. Correct fingerprint registration and input methods **12**
2. Introduction **14**
2.1. Features **14**
2.2. Configuration **16**
2.2.1. Network configuration 16
2.2.2. Standalone configuration 16
2.3. Specifications **17**
3. Device configuration settings **18**
3.1. Check items before device configuration settings **18**
3.1.1. Entering menu 18
3.1.2. Changing setting parameters 18
3.1.3. Saving device configuration settings 19
3.2. Menu configuration **20**
3.3. User account **22**
3.3.1. User registration 22
3.3.2. Deleting User 27
3.3.3. Modifying User 27
3.3.4. Administrator registration 30
3.3.5. Deleting All Users 30
3.4. Network settings **31**
3.4.1. Terminal ID settings 31
3.4.2. Connection [NS / SN / NO] mode settings 31
3.4.3. Connection configuration settings 32
3.4.4. IP address settings 32
3.4.5. Subnet mask settings 33
3.4.6. Gateway settings 33
3.4.7. Server IP settings 33
3.4.8. Server port settings 34
3.5. Option settings **35**
3.5.1. Application mode settings 35
3.5.2. Option settings for authentication 37
3.5.3. Doorlock settings 39
3.5.4. Volume settings 41
3.5.5. Current time settings 42

3.5.6. Other Setting 43
3.6. Terminal information view 44
3.7. Extra functions 45
3.7.1. Terminal lock settings 45
3.7.2. Reading card number 45
3.8. Device settings 46
3.8.1. System configuration settings 46
3.8.2. Function key settings 47
3.8.3. Card reader settings 47
3.8.4. Fingerprint sensor settings 48
3.8.5. Wiegand output settings 49
3.8.6. Terminal initialization 50
4. How to use the terminal 52
4.1. Access control 52
4.1.1. Authentication mode 52
4.1.2. [1:1] fingerprint authentication 53
4.1.3. [1:N] fingerprint authentication 54
4.1.4. Password authentication 55
4.1.5. Card authentication 56
4.1.6. User ID group authentication 57
4.1.7. Multiple fingerprint authentication 58
4.2. Time & Attendance control 59
4.2.1. Authentication mode 59
4.2.2. [1:1] fingerprint authentication 59
4.2.3. [1:N] fingerprint authentication 60
4.2.4. Password authentication 60
4.2.5. Card authentication 60
4.2.6. User ID group authentication 60
4.2.7. Expansion of working mode by multi-key function 60
4.3. Meal control 61
4.3.1. Meal classification 61
4.3.2. [1:1] fingerprint authentication 62
4.3.3. [1:N] fingerprint authentication 62
4.3.4. Password authentication 62
4.3.5. Card authentication 62
4.3.6. User ID group authentication 62
4.3.7. Double authentication 62

1. Before use

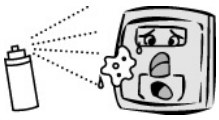
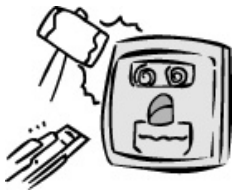
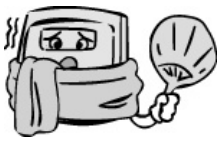
1.1. Safety precautions

- Warning

Handling with wet hands or allowing liquid to flow into it is prohibited. -> It may cause an electric shock or damage.		Do not place a fire source near the terminal. -> It may cause a fire.	
Do not disassemble, repair, or modify the terminal at discretion. -> It may cause an electric shock, fire or damage.		Keep out of reach of children. -> It may cause an accident or damage.	

- If the above warning is ignored, it may result in death or serious injury.

- Caution

Keep away from direct sunlight -> It may cause deformation or color change.		Avoid high humidity or dust -> The terminal may be damaged.	
Avoid using water, benzene, thinner, or alcohol for cleaning -> It may cause an electric shock or fire.		Do not place a magnet close to the terminal. -> The terminal may break down or malfunction.	
Do not contaminate the fingerprint input area. -> Fingerprints may not be well recognized.		Avoid using insecticide or flammable spray near the terminal. -> It may result in deformation or color change.	
Avoid impacts or using sharp objects on the terminal. -> The terminal may be damaged and broken.		Avoid severe temperature changes -> The terminal may be broken.	

- If the above cautions are ignored, it may result in property loss or human injury.

※ Under no circumstances will UNION COMMUNITY be responsible for accidents or damages caused by inappropriate use of the product without referring to the user manual.

1.2. Terminal description

LED Lamp : terminal operation status

- PWR : ON when VIRDI 3000 is under normal operation
- DOOR: Yellow LED is on when successful authentication makes electronic door open/close unit open. Red LED is on when terminal cover is opened.

Mic :
Connect to doorphone

LCD display window :
Display character message for all the operations

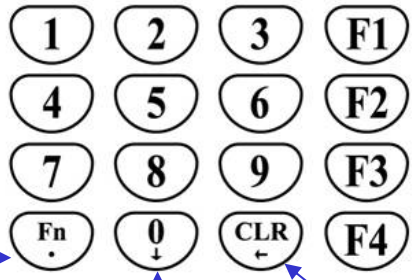
Fingerprint input window :
Window for fingerprint input

Speaker :
explanation of operation status and communication with doorphone

Card input position
: Option

Keypad : Enter numbers for environment setting or authentication ID input

1.3. Button description



start

leave

outside work

come back to company

Terminal menu setting (Enters into menu mode for terminal menu setting when pressed over 2 seconds.)

Enter '0' or LCD menu scroll

Clear typo when entering settings
Move up to higher menu
Use when escaping from menu setting

Visitors use this to ring the doorphone bell

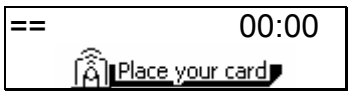
Use after entering the settings when configuring the terminal environment

1.4. Operation screen description

== connected to network server
→← disconnected to network server

Access mode display in case of access control (F1, F2, F3, F4)
T&A mode display in case of time & attendance control(START, LEAVE, OUT, BACK, NORMAL)
Successful authentication number for mealtime in case of meal control (MENU-1, MENU-2, MENU-3, MENU-4)

== 00:00 VIRDI 3000	- Initial screen
== 00:00 Input ID	- Waiting for a user's ID to be input
== 00:00 Input FP	- Fingerprint input
== 00:00 password	- Password input
== 00:00 Success	- Successful authentication
== 00:00 Matching fail	- Authentication failed
== 00:00 Unregistered	- When a non-registered user ID is entered - When connection mode is SN and 1:N identification is tried even though there is no user allowed for 1:N identification
== 00:00 Duplicate!	- When the terminal is under meal control mode and a user tries more than two time authentication during the same mealtime
== 00:00 Net Error	- There is no response from the server during the authentication process. - Network to server is disconnected during the authentication process.
→← 00:00 Connecting	- There is no user registered on the terminal or no connection to the server, so it is trying to connect.

	- Waiting for card to be input
	- A registered user tried authentication at that time when access is not allowed.
	- Waiting for a reply from the server for authentication
	- Terminal is locked - It is not mealtime in case of meal control mode
	- Terminal program is in upgrade **(Power must not turn off when this message is displayed.)**

1.5. Voice information during operation

"Please enter your fingerprint"	Enter fingerprint using the fingerprint input window
"You are authorized"	Successful authentication
"Please try again"	Authentication failed

1.6. Buzzer sound during operation

"ppig"	When a button is pressed or a card is being read When fingerprint input is completed and user is allowed to take off his fingertip
"ppibig"	Authentication is failed or wrong user fingerprint input happened
"ppiriririck"	Waiting for fingerprint input
"ppiririck"	Authentication is successful or settings for the current user are completed

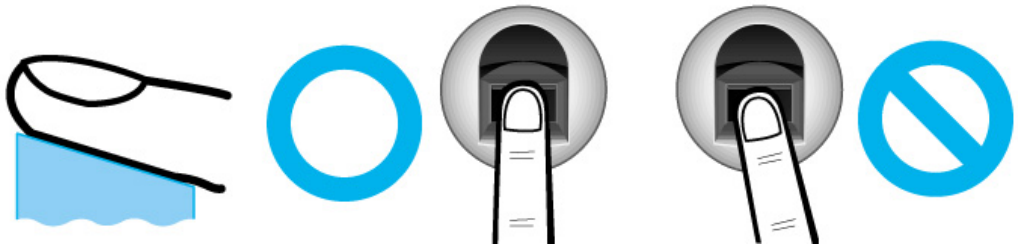
1.7. LED signal during operation

PWR ●	Power On/Off
DOOR ● [Two color LED] ●	Shows door status like Open or Close. When door is open, it(green) is on. Shows terminal status. When terminal cover is open, it(red) is on.

1.8. Correct fingerprint registration and input methods

- Correct fingerprint registration methods

  Place your index finger on the window just as you do with a finger stamp.
  Finger tip touching is not an appropriate registration or input method.
  Make sure the center of your finger touches the window.



- Use your index finger, if possible.

  As usual, the index finger guarantees an accurate and stable fingerprint input.

- Check if your fingerprint is unclear or damaged.
  It is tricky to recognize fingerprints on dry, wet, unclear, or injured fingers. Use another finger in this case.

- Cautions about fingerprint condition

  Depending on the user's fingerprint condition, some fingerprints may not be used or may cause an inconvenience.

  - If the fingerprint is damaged or very unclear, then it cannot be recognized. Please use a password instead in this case.
  - When a finger is dry, breathe on the finger for smooth operation.
  - For kids, it may be tricky or impossible to use the terminal because their fingerprints are too small or very unclear. It is recommended to register their fingerprints every six months.
  - For the elderly, it may not be possible to register their fingerprints if there are too many fine lines on the fingerprints.
  - If fingerprints are very unclear, it may be convenient if you register 2~3 fingerprints.
  - It is recommended that you register more than 2 fingerprints.

2. Introduction

2.1. Features

- Access control system using LAN
  - Communication between the unit and authentication server is done through a UTP cable and TCP/IP protocol, so an existing LAN can be used as it is. It guarantees network-based administration and monitoring as well as easy expansion, high reliability, and higher speed.

- Convenient Auto Sensing function
  - Simple authentication process without any key input; simple fingerprint touching is sufficient.

- Simple authentication using fingerprints
  - Fingerprint authentication technology prevents users from forgotten password or card, stolen key or card, etc., which is one of good ways to improve security level.

- High processing capacity of terminal and server
  - There is not any limit on management of users' access information in case that access server is used. Even in standalone operation by using local terminal, it is possible to manage fingerprint authentication of more than 8,000 users (in optional case).

- Various information messages
  - It ensures easy fingerprint recognition because voice and LCD window information are provided during the authentication process. In addition, the backlight installed in the LCD window helps with easy key operation in the dark.

- Optional doorphone
  - Easy visitor identification and convenient response.

- Various and flexible access controls
  - No risk of rent, forgery, or loss of keys or cards
  - Perfect control by assigning different security clearances to each user or group
  - Flexibility provided by allowing limited time for entry/exit
  - Low maintenance
  - No need to issue visitor card for visitor

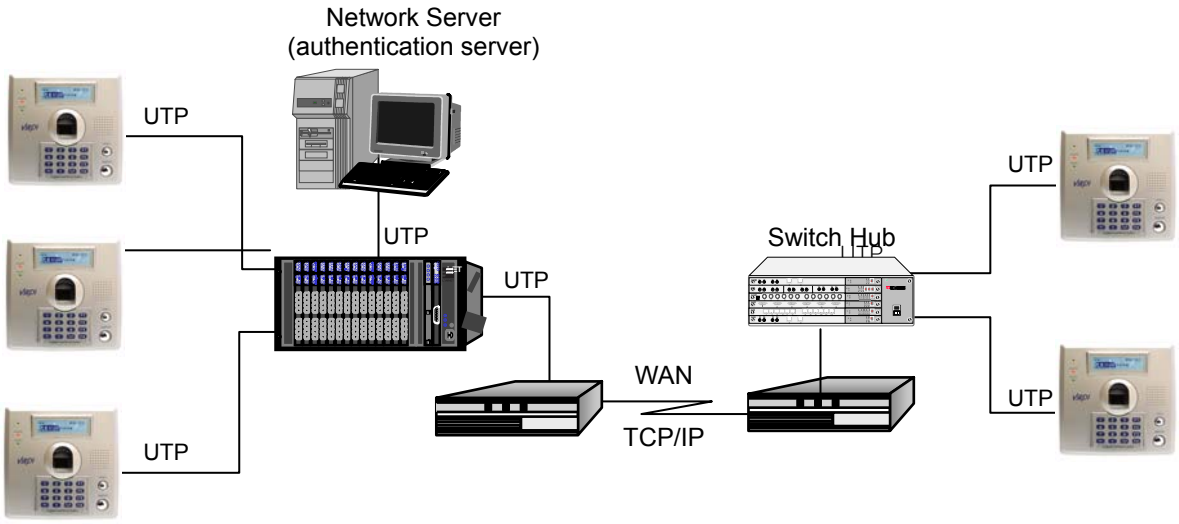
- Various applications including access control, time & attendance, meal control, etc.
  - Various operation modes depending on the terminal menu settings

- Various registration and authentication methods
  - There are a total of 11 registration and authentication methods (4 methods if the card reader is not installed), so you are required to select one method before registering users and an administrator.

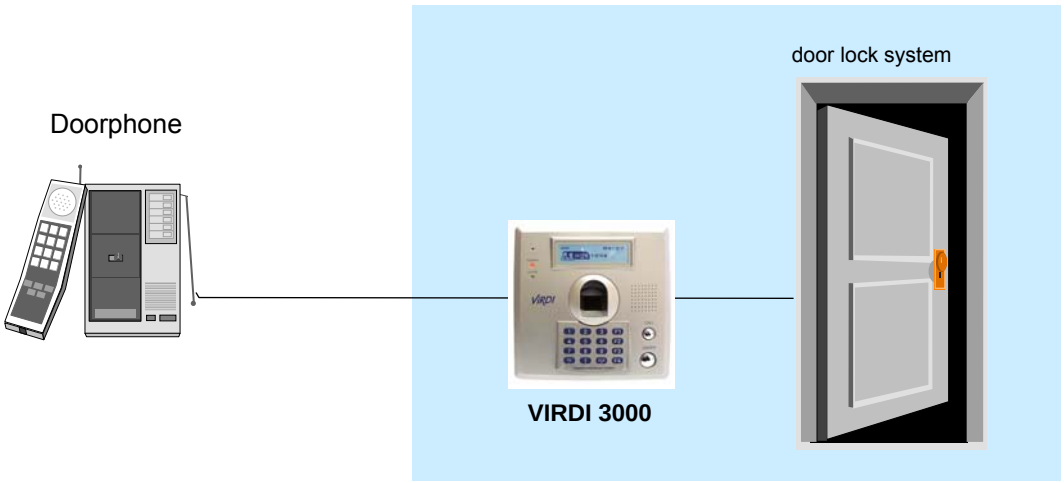
FP	Fingerprint registration Fingerprint authentication
ID&PW	Password registration Password authentication after ID input
FP|PW	Fingerprint and password registration Fingerprint or password authentication
FP&PW	Fingerprint and password registration Password authentication after fingerprint authentication
RF	Card registration Card authentication
RF|FP	Card and fingerprint registration Card or fingerprint authentication
RF&FP	Card and fingerprint registration Fingerprint authentication after card authentication
RF|PW	Card and password registration Card or password authentication
RF&PW	Card and password registration Password authentication after card authentication
ID&FP|RF&FP	Card and fingerprint registration Fingerprint authentication after ID input or fingerprint authentication after card authentication
ID&PW|RF&PW	Card and password registration Password authentication after ID input or password authentication after card authentication

2.2. Configuration

2.2.1. Network configuration



2.2.2. Standalone configuration



2.3. Specifications

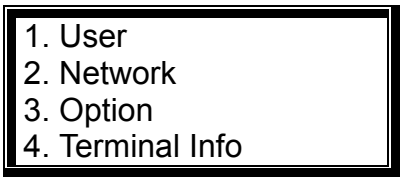
ITEM	SPEC	REMARK
CPU	32-Bit RISC CPU (266MHz)	
MEMORY	8M SDRAM	
	4M FLASH (Default)	3,520 fingerprints
	8M FLASH (Option)	8,160 fingerprints
Fingerprint sensor	Optical	
Authentication speed	<1 sec.	
Scan Area / Resolution	12.9 * 15.2mm / 500 DPI	
FRR / FAR	0.1% / 0.001%	
Communication Port	TCP/IP, RS-232, Wiegand	
	RS-485 (Option)	
Temperature / Humidity	-10~50 / Lower than 90% RH	
LCD	122 X 32 Graphic LCD	
SIZE	137 X 137 X 50mm	
AC / DC Adapter	INPUT: Universal AC 100~250V	
	OUTPUT: DC 12V (Option: DC 24V)	
	UL, CSA, CE Approved	
Options	RF Card Reader	EM Card, 125kHz
	Smart Card Reader	A-type, 13.56MHz
	Door phone	

3. Device configuration settings

3.1. Check items before device configuration settings

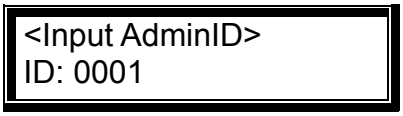
3.1.1. Entering menu

The following screen appears when the [Fn] button is pressed for over 2 sec.



Press [0] to view menus not shown in the LCD window.

Press a number key in order to go submenu. The following administrator authentication allows for entry of submenu.



Press [ENTER] after entering the administrator's ID, and the administrator authentication is processed according to the previous setting such as fingerprint authentication or password authentication. If the authentication succeeds, submenu screen appears.

※ Administrator authentication is required only once for all in main menu, so all other menus are accessible until he/she completely exits from the main menu.

3.1.2. Changing setting parameters

To change setting parameters, press the [CLR] button to delete old values and input new values.

Press [0] to see menus not shown in the LCD window, and press the corresponding number to select a menu.

Press [ENTER] for confirmation of setting parameter or to move to the next setting, and press the [CLR] button to move to upper menus.

Hold the [CLR] button for over 2 sec. to cancel the current setting and move to the upper menu.

3.1.3. Saving device configuration settings

Press the [CLR] button in the main menu to save device configuration settings. The following screen appears

Save? [Y=1/N=2]:_

Press [1] to save changes. If not, press [2].

- If there are no changes in device configuration settings, it goes out of this setting mode without going through the above screen.
- If there is no input for a certain period of time while changing the device configuration settings, the setting process finishes. If there are changes in device configuration settings, the above screen "Save?" appears. If not, it goes out of this setting mode and the initial screen appears.

3.2. Menu configuration

1. User	1. Add 2. Delete 3. Modify 4. Add Admin 5. Delete All	
2. Network	1) Terminal ID 2) Mode [NS/SN/NO] 3) Network Type [Static IP/DHCP] 4) IP Address 5) Subnet Mask 6) Gateway 7) Server IP 8) Server port	
3. Option	1. Application [Access/Time Attendance /Meal]	<Application> <Start Time> <Leave Time> <Normal Time> <Multi Fn-Key>
	2. Verify Option	<Show User ID> <Auto Enter Key> <Only Card> <Enable 1:N> <User ID Group> <Verify Multi-FP>
	3. Set Doorlock	<Door Monitor> <Open Duration> <Door Open Alarm>
	4. Sound Control	<Use Voice> <Beeper Volume> <Case Open Alarm>
	5. Time Setting	
	6. Other Setting	<LCD Backlight>

4. Terminal Info	Terminal ID=0001 Version=10.41.00 Application=Access Language=English Mode=NS Network Type= Static(1) Mac-Address=000265201111 IP Address=192.168.0.3 Gateway=192.168.0.1 Subnet Mask=255.255.255.0 Server IP=192.168.0.2 Svr-Port=2204 Card Reader=None FP-Sensor= FOS01 1:1 Level=4 1:N Level=5 Max User=0 MAX FP=0 All User=0 All Admin=0 All FP=0 1:N User=0 1:N FP=0 All Log=0	
5. Ext functions	1. Lock Terminal 2. Read Card No.	
6. Device	1. System Config	<ID Length> <Language>
	2. Set Fn-Key	
	3. Card Reader	
	4. FP-Sensor	<1:1 Level> <1:N Level> <I-Capture>
	5. Wiegand	
	6. Initialize	1. Init Config 2. Delete Log 3. Init Terminal

3.3. User account

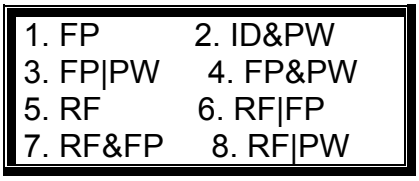
3.3.1. User registration

Press the [1] button in the main menu to select "1.User", and the following screen appears:

Press [1] to register a new user.

Enter a new user ID, and press [ENTER].

If the entered ID already exists, it moves to the upper menu with a "ppibig" sound. If not, selection screen for the following authentication method appears:



Press [0] to see menus not shown in the LCD window. Select one from among the 11 registration methods.

3.3.1.1. "1. FP" registration

Fingerprint registration and fingerprint authentication

◆ [Fn] → [1] → [1] → User ID [ENTER] → [1] → 1:1 Level [ENTER]
→ Enable 1:N [ENTER] → Input FP → Input the same FP again ◆

Recommended setting: '0'

Different authentication levels can be assigned to respectively different users. If the authentication level for a user is set to [0], the authentication level for the terminal is applied to the user. Therefore, if the 1:1 authentication level of the terminal is changed, the applied authentication level for all users respectively set to '0;'is simultaneously changed.

Press [ENTER] to move to the next setting.

<Enable 1:N> (N=0/Y=1): 0	The default is '0'. To enable 1:N authentication, it should be set to '1'.

In case that there are not many users or for the convenience of a specific user, a fingerprint only without ID can be used for authentication. For authentication without ID, it shall be set to '1'. For authentication with ID, it shall be set to '0'.

Press [ENTER] to enter relevant fingerprints.

<Add FP> Input Your FP

A "ppiriririck" buzzer sound rings twice and a light on the fingerprint sensor turns on. Place a finger onto the fingerprint input window and wait for 2~3 seconds until the light turns off and the fingerprint is saved.

Please note that the same fingerprint must be inputted twice. To enter the same fingerprint again, remove the finger from the window and place the same finger again onto the window.

If registration succeeds, a "ppiririck" buzzer sound rings. Then, it returns to the "1.Add" screen. If the fingerprint image is not in good conditions or there is no input in the window for 10 seconds after the fingerprint sensor light turns on, it returns to the "1. Add" screen with a failure buzzer sound "ppibig".

In case that the fingerprint to be registered is in bad conditions, repeat to try the registration process more than 2 or 3 times or register other fingerprint. For remarkably few people having fingerprints in bad conditions which are not properly accepted for registration process, it is recommended to use a password for authentication.

3.3.1.2. "2. ID&PW" registration

Password registration and password authentication for a user

◆ [Fn] → [1] → [1] → User ID [ENTER] → [2] → Input PW [ENTER] → Input same PW [ENTER] ◆

<Input PW> PW: _ _ _ _ _ _ _ _	Input password. Password should be 1~8 characters in length.

Press [ENTER] to input the password.

<Confirm PW> PW: _ _ _ _ _ _ _ _

Input the same password once more for confirmation.

If registration succeeds, a "ppiririck" buzzer sound rings. Then, it returns to the "1.Add" screen. If they are different, a "ppibig" buzzer sound indicating failure rings and the "1.Add" menu screen appears.

3.3.1.3. "3. FP|PW" registration

After both fingerprint and password are registered, authentication method is selectable during fingerprint or password.

◆ [Fn] → [1] → [1] → User ID [ENTER] → [3] → Input PW [ENTER]
→ Input same PW [ENTER] → 1:1 Level [ENTER] → Enable 1:N [ENTER]
→ Input FP → Input the same FP again◆

As mentioned above, password registration (refer to ② "2. ID&PW" registration) precedes fingerprint registration (refer to ① "1. FP" registration).

3.3.1.4. "4. FP&PW" registration

After both fingerprint and password are registered, fingerprint authentication and password authentication should be done for access. Fingerprint authentication precedes password authentication.

◆ [Fn] → [1] → [1] → User ID [ENTER] → [4] → Input PW [ENTER]
→ Input same PW [ENTER] → 1:1 Level [ENTER] → Enable 1:N [ENTER]
→ Input FP → Input same FP ◆

3.3.1.5. "5. RF" registration

Card registration and card authentication

◆ [Fn] → [1] → [1] → User ID [ENTER] → [5] → Place the card ◆

<Add Card> Place Your Card

To cancel registration, press the [CLR] button.

If a user places the card close to the unit, a "ppiririck" buzzer sound rings in case of successful registration. "1. Add" menu appears.

3.3.1.6. "6. RF|FP" registration

After both card and fingerprint are registered, authentication method is selectable during card or fingerprint.

◆ [Fn] → [1] → [1] → User ID [ENTER] → [6] → Place the card →
1:1 Level [ENTER] → Enable 1:N [ENTER] → Input FP → Input same FP ◆

Card registration (refer to ⑤ "5. RF" registration) precedes fingerprint registration (refer to ① "1. FP" registration).

3.3.1.7. "7. RF&FP" registration

After both card and fingerprint are registered, card authentication and fingerprint authentication should be done for access. Card authentication precedes fingerprint authentication.

◆ [Fn] → [1] → [1] → User ID [ENTER] → [7] → Place the card →
1:1 Level [ENTER] → Enable 1:N [ENTER] → Input FP → Input same FP ◆

Card registration (refer to ⑤ "5. RF" registration) precedes fingerprint registration (refer to ① "1. FP" registration).

3.3.1.8. "8. RF|PW" registration

After both card and password are registered, authentication method is selectable during card or password.

◆ [Fn] → [1] → [1] → User ID [ENTER] → [8] → Place the card
→ Input PW [ENTER] → Input same PW [ENTER] ◆

Card registration (refer to ⑤ "5. RF" registration) precedes password registration (refer to ② "2. ID&PW" registration).

3.3.1.9. "91. RF&PW" registration

After both card and password are registered, card authentication and password authentication should be done for access. Card authentication precedes password authentication.

◆ [Fn] → [1] → [1] → User ID [ENTER] → [9][1] → Place the card
→ Input PW [ENTER] → Input same PW [ENTER] ◆

Card registration (refer to ⑤ "5. RF" registration) precedes password registration (refer to ② "2. ID&PW" registration).

3.3.1.10. "92. ID&FP|RF&FP" registration

After both card and fingerprint are registered, authentication method is selectable during ID and fingerprint authentication or card and fingerprint authentication.

◆ [Fn] → [1] → [1] → User ID [ENTER] → [9][2] → Place the card → 1:1 Level [ENTER] → Enable 1:N [ENTER] → Input FP → Input same FP ◆

If a user feels difficult in inputting ID, a card can be used instead of ID input for authentication.

Card registration (refer to ⑤ "5. RF" registration) precedes fingerprint registration (refer to ① "1. FP" registration).

3.3.1.11. "93. ID&PW|RF&PW" registration

After both card and password are registered, authentication method is selectable during ID and password authentication or card and password authentication.

◆ [Fn] → [1] → [1] → User ID [ENTER] → [9][3] → Place the card → Input PW [ENTER] → Input same PW [ENTER] ◆

If a user feels difficult in inputting ID, a card can be used instead of ID input for authentication.

Card registration (refer to ⑤ "5. RF" registration) precedes password registration (refer to ② "2. ID&PW" registration).

3.3.2. Deleting User

◆ [Fn] → [1] → [2] → User ID [ENTER] ◆

In the main menu, press [1] to select "1.User", and the following screen appears:

To delete user, press [2].

After entering the user ID to be deleted, press [ENTER]. All the information about the user in the local terminal is deleted together with a "ppiririck" buzzer sound. However, the information about the user is still stored in the server. To completely delete this information, the data in the server should be deleted.

If a non-registered user ID is entered, "2.Delete" appears together with a "ppibig" sound.

Caution is required when deleting a user or an administrator as there is no differential procedure for deleting their information. Also, carefully note that user's information stored just in the local terminal – not in the server –is not recoverable after deletion is completely done.

3.3.3. Modifying User

◆ [Fn] → [1] → [3] → User ID [ENTER] → Select the menu number for modification → Modify relevant value ◆

In the main menu, press [1] to select "1. User" to see the following screen:

To Modify a user, press [3].

Enter the user's ID to modify, and press [ENTER].

There is no difference for modifying general user's or administrator's information.

3.3.3.1. "1. FP" user

As for users who registered only their fingerprints for access, they can modify 1:1 authentication level and add other fingerprints.

1. 1:1 Level 2. Add FP

To change the authentication level, press [1]. To add a fingerprint to the corresponding ID, press [2].

※ A maximum of 5 fingerprints can be added to an ID. If there is an attempt to add more than 5 fingerprints, a "ppibig" buzzer sound rings when [2] is pressed.

[1] When modifying 1:1 authentication level is selected

<1:1 Level> (0-9): 0

Recommended setting: '0'

To change this value, press the [CLR] to delete the current value and enter the new value.

[2] When registering additional fingerprints is selected

<Add FP> Input Your FP

This is same as 'Add FP' in 3.3.1.1. "1. FP" registration. The same fingerprint must be inputted twice.

If additional fingerprint registration succeeds, a "ppiririck" buzzer sound rings. If not, a "ppibig" buzzer sound rings and the "1. Add" menu appears.

3.3.3.2. "2.ID&PW" user

When a user wants to change his/her password

1. Modify PW

To change passwords, press [1]. To cancel this operation, press [CLR].

Press the [1] button to modify the passwords

<Input PW> PW: _ _ _ _ _ _ _ _

Input password. Password should be 1~8 characters in length.

Press [ENTER] after inputting the password.

<Confirm PW> PW: _ _ _ _ _ _ _ _

Input the same password once more for confirmation.

Press [ENTER] to confirm the password.

If password modification succeeds, a "ppiririck" buzzer sound rings. If not, a "ppibig" buzzer sound rings and the "1. Add" menu appears.

3.3.3.3. "3.FP|PW", "4.FP&PW" user

1. 1:1 Level 2. Add FP 3. Modify PW

Press [0] to see menus not shown in the LCD window.
To cancel, press the [CLR] button.

Press the [1] button to change the 1:1 Level (refer to "3.3.3.1")
Press the [2] button to register additional fingerprints (refer to "3.3.3.1")
Press the [3] button to change passwords (refer to "3.3.3.2").

3.3.3.4. "5.RF" user

1. Change Card

To change the card, press [1].
To cancel, press the [CLR] button.

Press the [1] button to change the card.

<Change Card> Place Your Card

To cancel, press the [CLR] button.

If a user places the card close to the unit, a "ppiririck" buzzer sound in case of successful modification rings and the "1. Add" menu appears.

3.3.3.5. "6.RF|FP", "7.RF&FP", "92.ID&FP|RF&FP" user

1. 1:1 Level 2. Add FP 3. Change Card

Press [0] to see menus not shown in the LCD window.
To cancel, press the [CLR] button.

Press the [1] button to change the 1:1 Level (refer to "3.3.3.1")
Press the [2] button to register additional fingerprints (refer to "3.3.3.1")
Press the [3] button to change the card (refer to "3.3.3.4").

3.3.3.6. "8.RF|PW", "91.RF&PW", "93.ID&PW|RF&PW" user

1. Modify PW 2. Change Card

Press the [1] button to change passwords (refer to "3.3.3.2").
Press the [2] button to change the card (refer to "3.3.3.4").

3.3.4. Administrator registration

◆ [Fn] → [1] → [4] → Admin ID [ENTER] ◆

In the main menu, press [1] to select "1.User", and the following screen appears:

1. Add 2. Delete 3. Modify 4. Add Admin

For administrator registration, press [4].

Admin ID [NEW] ID: _ _ _ _

Enter the administrator ID to register and press [ENTER].

※ The procedures for administrator registration are the same as those for user registration.

Be careful to register new administrator as the registered administrator can change the terminal configuration settings including registration/modification/deletion of user information.

3.3.5. Deleting All Users

◆ [Fn] → [1] → [5] ◆

In the main menu, press [1] to select "1. User". By using the button [0], you can scroll the unseen menu.

5. Delete All

To delete all users, press [5].

Delete All? [Y=1/N=2]: _

To delete all users, press [1]. If not, press [2].

Special care is required because all user accounts including the administrator are deleted with this operation.

When this operation succeeds, a "ppiririck" buzzer sound rings and the "1. Add" menu appears.

3.4. Network settings

In the main menu, press [2] to select "2.Network" to see the following screen. When this setting is done, press [ENTER] to move to the next setting.

3.4.1. Terminal ID settings

◆ [Fn] → [2] ◆

< Terminal ID > ID: 00000001

This ID is unique for each terminal and used by an authentication server to distinguish each terminal. The default is "00000001". It should be identical to the door ID set in the server program and its length should be 1~8 characters. If the terminal ID is "1000", enter [1][0][0][0] in sequence. If it is "0001", enter only [1]. Press [ENTER] to move to the next setting.

3.4.2. Connection [NS / SN / NO] mode settings

◆ [Fn] → [2] → [ENTER] ◆

Mode [NS / SN / NO] (0-2): 0

NS mode: '0', SN mode: '1' and NO mode: '2'

This defines where the priority for authentication is between the local terminal and network server, and the default is '0' (NS). There are three different modes as follow:

- NS mode: select [0]. If the local terminal is properly connected to network server, authentication is done in the server. In case of disconnection between local terminal and network server due to network troubles or others, it is done in the local terminal.

- SN mode: select [1]. Even though the local terminal is properly connected to network server, the authentication is done in the local terminal and its result is transmitted to network server in real time.
  However, if the user ID entered for 1:1 authentication does not exist in the local terminal, the relevant authentication is tried in network server.

- NO mode: select [2]. The authentication operation is done only in network server.

Depending on number of terminals, number of users, or network conditions, each different mode can flexibly be used. But if there are more than 10 terminals connected to the server for simultaneous authentication or there are frequent network problems, it is recommended to use "SN" authentication (setting [1]).

Press [ENTER] to move to the next setting.

3.4.3. Connection configuration settings

◆ [Fn] → [2] → [ENTER] → [ENTER] ◆

Network Type:0 0:Static 1:DHCP	Press [0] for Static IP. Press [1] for DHCP.

The default is "0: Static IP". If a static IP is assigned to the terminal from present network system, press [0]. If there is a DHCP server in network system from which a dynamic IP is assigned to the terminal, press [1].

Press [ENTER] to move to the next setting.

※ For Static IP settings, refer to '3.4.4. IP address', '3.4.5. Subnet mask' and '3.4.6. Gateway'. In case of dynamic IP, there is no need for additional settings.

3.4.4. IP address settings

<IP Address> 192.168.0.3	Press [CLR] to delete an old IP and enter the new IP.

If the IP address is '210.98.100.50', enter as below:

[2] [1] [0] [FN] [9] [8] [FN] [1] [0] [0] [FN] [5] [0]

Press [ENTER] to move to the next setting.

3.4.5. Subnet mask settings

<Subnet Mask> 255.255.255.0

Press [CLR] to delete an old value and enter the new value.

If the subnet mask is '255.255.255.0', enter as below:

[2] [5] [5] [FN] [2] [5] [5] [FN] [2] [5] [5] [FN] [0]

Press [ENTER] to move to the next setting.

3.4.6. Gateway settings

<Gateway> 192.168.0.1

Press [CLR] to delete an old value and enter the new value.

If the gateway IP address is '210.98.100.1', enter as below:

[2] [1] [0] [FN] [9] [8] [FN] [1] [0] [0] [FN] [1]

Press [ENTER] to move to the next setting.

3.4.7. Server IP settings

< Server IP > 192.168.0.2

Press [CLR] to delete an old value and enter the new value.

If the sever address is '210.98.100.121', enter as below:

[2] [1] [0] [FN] [9] [8] [FN] [1] [0] [0] [FN] [1] [2] [1]

Press [ENTER] to move to the next setting.

3.4.8. Server port settings

< Server port >
Num: 2201

Press [CLR] to delete an old value and enter the new value.

As the port number of the authentication server, the default is 2201. Special care is required when changing this number because the corresponding number in the server should also be changed with the same number.

If the server port is '2201', enter as below:
[2] [2] [0] [1]

After the network setting is completely done, press [ENTER] to return to the main menu.

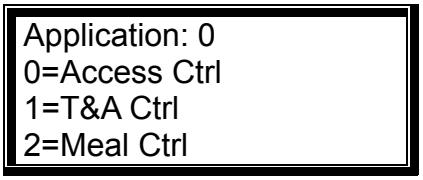
3.5. Option settings

3.5.1. Application mode settings

In the main menu, press [3] to select "3. Option" and following screen appears:

To set the basic operation mode of a terminal, press [1].

◆ [Fn] → [3] → [1] ◆



The default is '0=(Access Ctrl)'.

For access control application, set as [0], for time & attendance, set as [1] and lastly, for meal control, set as [2].

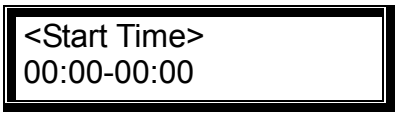
Press [ENTER] to move to detailed settings for each application mode.

3.5.1.1. [0]: Access Control

There are no detailed settings under access control application here. It moves to the upper menu.

3.5.1.2. [1]: Time Attendance control

By setting up those default times regarding Start/Leave/Out/Back, the terminal display mode after authentication can be automatically changed to programmed time & attendance mode. In addition, by using multi-Fn key, over 40 sub modes of time & attendance can be defined.



If time setting is not necessary, set as '00:00-00:00'.

To change the start time from 00:00~00:00 to 06:00~09:59, press [CLR] to delete the existing setting time, and enter [0][6][0][0][0][9][5][9] in sequence.

As long as no other function button is pressed during the setting time, it operates in start time mode. Even if the authentication for outside work (Out) happens by pressing [F3] function key, the terminal display mode after the authentication of outside work is automatically changed to start time mode, which is very convenient for users in time & attendance mode.

After setting <start time>, set <leave time> and <normal time> in the same manner. Note that each time must not overlap.

Ex.)start time:06:00~09:59, leave time:17:00~22:00 and normal time:10:00~16:59

< Start Time >	< Leave Time >	< Normal Time >
06:00~09:59	17:00~22:00	10:00~16:59

After lastly setting normal time, press [ENTER] to see the "Multi Fn-key" setting menu, which allows more than 5 time & attendance modes.

<Multi Fn-key>
1=F1: X 2=F2: X
3=F3: X 4=F4: X

Default setting: all 'X'

This menu is useful when more than 5 time & attendance modes are necessary.

- When setting as X: each function key represents a specific working mode such as F1=Start, F2=Leave, F3=Outside work (out) and F4=Back. When a function key is pressed, authentication mode is changed to the corresponding working mode.
- When setting as O: a mode is defined by the combination of a function key and a number key such as "F3+1". For example, if the setting is 1=F1: X 2=F2: X 3=F3: X 4=F4: O, 14 different working modes can be defined according to user input such as [ENTER]: normal, [F1]: start, [F2]: leave, [F3]: outside work (out), and [F4]+'0'~[F4]+'9'.

The O/X setting can be changed by pressing the corresponding number key. After setting is completed, press [ENTER] to move to the upper menu.

3.5.1.3. [2]: Meal Control

<Breakfast >
00:00-00:00

If time setting is not necessary, set it as 00:00-00:00.

This is the setting for breakfast, so every authentication during this assigned time is considered for breakfast. After setting breakfast time, set <Lunch time>, <Dinner time>, <Supper time>, and <Snack time> in sequence. Set it to 00:00-00:00 if the corresponding meal time is not used.

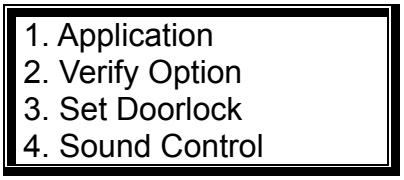
Each time period must not overlap. Only one time authentication is possible for each user in each time period. If double authentication or more for each time period is required, place a finger or a card for authentication while pressing [ENTER].

If a time period is not set for a meal time, the terminal displays a "lock setting!" message. All inputs are blocked except for entering menu mode once the terminal is locked.

After setting <Snack time>, press [ENTER] to move to the upper menu.

3.5.2. Option settings for authentication

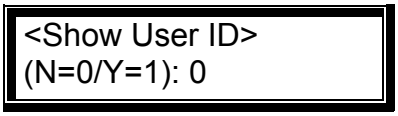
In the main menu, press [3] to select "3. Option" and the following screen appears:



To set the basic option for authentication, press [2].

3.5.2.1. Settings for ID display when authentication is successful

◆ [Fn] → [3] → [2] ◆



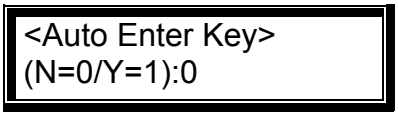
Default setting: '0'

If it is set to the default setting [0], only the "Success" message is displayed. If it is set to [1], user ID is displayed in the LCD window when authentication is successful as shown below:
(Ex.) OK! <0001>

Press [ENTER] to move to the next setting.

3.5.2.2. Auto enter key setting

◆ [Fn] → [3] → [2] → [ENTER] ◆



Default setting: '0'

If it is set to default setting [0], after input of ID, press [F1] ~ [F4], [Enter] or place a relevant finger for authentication. But if it is set to [1], after input of ID, users using password go to password authentication mode without pressing any function keys. In this case, the currently working mode is applied to the

authentication mode.

Press [ENTER] to move to the next setting.

3.5.2.3. Settings for only card authentication

◆ [Fn] → [3] → [2] → [ENTER] ◆

<Only Card> (N=0/Y=1): 0

Default setting: '0'

Even if a user is registered to be authenticated with a card & password or a card & fingerprint, if it is set to [1], a user can get access to an area through the relevant terminal only by using a card.

This function is useful at building entrance door – among other places of a building with several installed terminals - where there is frequent entrance and exit and there is no need for severe access control.

Press [ENTER] to move to the next setting.

3.5.2.4. 1:N authentication settings

◆ [Fn] → [3] → [2] → [ENTER] → [ENTER] ◆

<Enable 1:N> (N=0/Y=1): 0

Default setting: '1'

This enables fingerprint authentication without inputting a user ID or placing a card. For your information, even if a user is registered to be authenticated with 1:N authentication, only 1:1 authentication is allowed in the terminal if this is set to [0].

In cases that ID input or fingerprint authentication after placing a card – when card input replaces ID input – is unavoidably needed, it should be set to [0].

The followings are detailed settings about whether 1:N authentication is allowed or not.

① When 1:N authentication is allowed as setting of [1]

<User ID Group> (N=0/Y=1): 0

Default setting: '0'

If this setting is set to '1', inputting fore part of ID digits stands for a specific group, which speeds up 1:N authentication by searching for same fingerprint only among the specific group. This faster matching speed is very useful in case that over 1,000 users are registered.

If it is set to '1', as mentioned above, fingerprint matching is executed only among the user group starting with the same fore part of ID digits. If it is set to '0', inputted numbers is considered just as user's ID and only 1:1 authentication is executed.

For example, when a user ID is a 4-digit number and '12' is inputted for authentication, if it is set to '1', 1:N authentication is performed among user IDs '1200'~'1299'. If it is set to '0', 1:1 authentication only for user ID No. 12 is performed.

② When 1:N authentication is not allowed as setting of [0]

<Verify Multi-FP> (N=0/Y=1): 0

Default setting: '0'

If it is set to '1', for successful authentication, all registered fingerprints should be authenticated after ID (or card) input.

This is used when a high security level is required for special areas. If a user of 'ID 0001' has 3 fingerprints registered to the unit, all 3 fingerprints should be authenticated after ID input.

The authentication sequence for the 3 fingerprints does not matter in this case, but whole authentication fails if a single fingerprint is not successfully authenticated.

After the setting is completely done, press [ENTER] to move to the upper menu.

3.5.3. Doorlock settings

In the main menu, press [3] to select "3. Option" and the following screen appears:

1. Application 2. Verify Option 3. Set Doorlock 4. Sound Control

Press [3] for door settings.

3.5.3.1. Door opening time settings

◆ [Fn] → [3] → [3] ◆

<Open Duration> (00-30): 03

Default setting: '03' (unit: sec.)

This is used to set the door opening time after authentication is successfully done. This means the door opening time only for strike type but is not applicable to dead bolt type or auto door.

If this is set to [00], the door control in access control mode is out of control. Therefore, [00] setting may be possible only for time & attendance mode, where there is no need for lock control.

After this setting is completely done, press [ENTER] to move to the next setting.

3.5.3.2. Monitoring door status

◆ [Fn] → [3] → [3] → [ENTER] ◆

< Door Monitor> [0/1=NO/2=NC]: 0

Default setting: '0'

- '0': NW – No monitoring
- '1': NO – Dead bolt type or auto door
  (In case that lock monitoring pin is high when the door is locked)
- '2': NC - Strike type
  (In case that lock monitoring pin is low when the door is locked)

'0' setting is for no monitoring, '1' setting is for dead bolt type or auto door and '2' setting is for strike type. When this is set to '1' or '2', the door status through connected terminal is periodically transmitted to the server.

Once the setting is completely done, Press [ENTER] to move to the next setting.

3.5.3.3 Door open alarm settings

◆ [Fn] → [3] → [3] → [ENTER] → [ENTER] ◆

| < Door Open Alarm>
(00-30): 00 |
|---|

Default setting: '00'

The terminal checks if the door has been open for more than this setting time – from 5 seconds in minimum to 30 seconds in maximum. Opening for more than this setting time makes an alarm sound. If this is set to [00], there is no alarm sound. Even if it is set to '01' to '04', there is an alarm sound after the door has been open for 5 seconds in minimum.

There may be any unexpected troubles which make the door not closed. In this case, this alarm helps relevant persons (administrators) check what has caused the problem in a timely manner and eliminate the problem.

For smoothly operation of this setting, the relevant lock should be the lock type to be able to monitor whether the door is open or closed and its monitoring pin should properly be connected to the terminal. The previously mentioned setting for monitoring door status should be set to '1' or '2' for this operation.

Once the setting is completely done, press [ENTER] to move to the upper menu.

3.5.4. Volume settings

In the main menu, press [3] to select "3. Option", and the following screen appears:

| 1. Application
2. Verify Option
3. Set Doorlock
4. Sound Control |
|---|

Press [4] for volume settings.

3.5.4.1. Voice settings

◆ [Fn] → [3] → [4] ◆

| <Use Voice>
(N=0/Y=1): 1 |
|---|

Default setting: '1'

To make voice information about terminal available, set it to '1'. If not, set it to '0'. Press [ENTER] to move to the next setting.

3.5.4.2. Buzzer volume settings

◆ [Fn] → [3] → [4] → [ENTER] ◆

<Beeper volume> (0-2): 1

Default setting: '1'

This is for the terminal buzzer volume. If this is set to '0', there is no buzzer sound. '1' setting means low volume and '2' means high volume.

Press [ENTER] to move to the next setting.

3.5.4.3. Case open alarm settings

◆ [Fn] → [3] → [4] → [ENTER] → [ENTER] ◆

< Case Open Alarm> (N=0/Y=1): 0

Default setting: '0'

An alarm sounds if the terminal case is damaged or opened. For this setting, VIRDI 3000 series have case open sensor installed.

After the setting is completely done, press [ENTER] to move to the upper menu.

3.5.5. Current time settings

◆ [Fn] → [3] → [5] ◆

In the main menu, press [3] to select "3. Option". Press [5] to see the following screen:

<Time Setting> 20060401211806

This is to set the terminal current time. The above example represents the year 2006, month 04, date 01, hour 21, min. 18, and sec. 06. To change it, delete the old numbers with the [CLR] button before adding the new numbers.

Press [ENTER] to check that the current time is updated and move to the upper menu.

3.5.6. Other Setting

In the main menu, press [3] to select "3.Option". Press [6] to see the following screen:

5. Time Setting 6. Other Setting

Press [6] for other settings.

3.5.6.1. LCD Backlight On/Off settings

<LCD Backlight> (0=Off/1=On):

Default: '0'

◆ [Fn] → [3] → [6] ◆

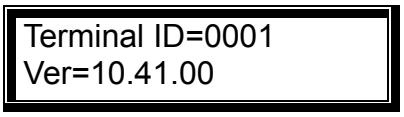
This is to set LCD backlight. If it is set to '1', LCD backlight is on all the times. On the other hand, if it is set to [0], the LCD backlight is normally off and keypad operation or placing a card makes the backlight on. Since it has passed 10 seconds after relevant operation is done, backlight becomes off.

After the setting is completely done, press [ENTER] to move to the upper menu.

3.6. Terminal information view

◆ [Fn] → [4] ◆

In the main menu, press [4] to select "4.Terminal info" and the following screen appears where all the environmental settings are displayed:



Press [0] to scroll up and down the screen.

Terminal ID	Terminal ID
Version	Terminal firmware version
Application	Terminal Application mode (Access/T&A/Meal)
Language	Language for text and voice of the LCD screen
Mode	Connection mode between terminal and network server
Network type	Network connection type (static IP/dynamic IP)
Mac Address	Terminal Ethernet hardware address
IP address	Terminal IP address
Gateway	Terminal gateway address
Subnet mask	Terminal subnet mask address
Server IP	IP address of network server connected to the terminal
Svr-port	Port number of network server program
Card Reader	Card reader type
FP-Sensor	Fingerprint sensor type
1:1 Level	Identification level for 1:1 authentication
1:N Level	Identification level for 1:N authentication
Max User	Maximum user capacity to be able to be registered to a terminal
Max FP	Maximum fingerprint capacity to be able to be registered to a terminal. For example, if there are 100 registered users and two fingerprints per user are registered, it means a total of 200 fingerprints is registered.
All User	Number of current users registered to a terminal including administrators
All Admin	Number of administrators registered to a terminal
All FP	Number of fingerprints currently registered to a terminal
1:N User	Number of users for 1:N authentication
1:N FP	Number of fingerprints for 1:N authentication
All Log	Authentication records stored in a terminal

3.7. Extra functions

In the main menu, press [5] to select "5.Ext functions" and the following screen appears:

```
1. Lock Terminal
2. Read Card No.
```

3.7.1. Terminal lock settings

◆ [Fn] → [5] → [1] ◆

```
<Lock?>
(N=0/Y=1): 0
```

Default setting '0': Releasing terminal lock
'1': Setting terminal lock

An administrator in local terminal – not by server program – can directly set up or release the terminal lock to the local terminal. If it is set to '1', the terminal is locked and nobody is accessible to the specific area through locked terminal until the administrator unlocks the terminal.

※ For this setting, 'Allow admin to access' in terminal configuration of server program should be permitted.

After the setting is completely done, press [ENTER] to move to the upper menu.

3.7.2. Reading card number

◆ [Fn] → [5] → [2] ◆

```
Place Your Card
```

This is an extra function which is not related to terminal configuration settings. By using this function, an administrator can read the card number when she/he places a card to the terminal mounted with card reader, in order to register the placed card to server. If this LCD screen pops up and then an administrator places a card to the terminal, the card number shows in the LCD screen.

To exit from this setting, press [CLR] to move to the upper menu.

3.8. Device settings

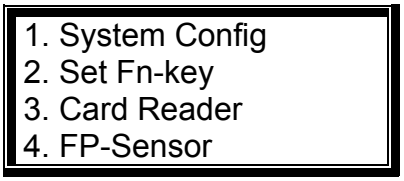
In the main menu, press [6] to select "6. Device" and the following screen asking for a password appears:

In most of cases, there is no need for modifying the device settings after installation. Therefore, be careful not to modify the device settings without any obvious reasons.

This previously set password from factory is to call administrator's attention, which is fixed one and should not be changed.

Input '084265' as the previously set password and press [ENTER] to show the detailed setting items.

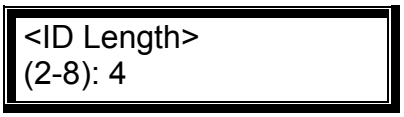
3.8.1. System configuration settings



Press [1] for system configuration settings.

3.8.1.1. User ID length settings

◆ [Fn] → [6] → "084265" [ENTER] → [1] ◆



Default setting: '4' digits

This ID length can be 2~8 digits and should be the same as that of ID registered in the server program. If the ID registered in the server program is '000075', input 6.

With modifying this ID length shorter than before during normal operation after installation, an administrator may not be able to be authenticated and enter into main menu if she/he has longer ID length, compared to the modified ID length. Therefore, be careful to give serious consideration before modifying the ID length.

Press [ENTER] to move to the next setting.

3.8.1.2. Language settings

◆ [Fn] → [6] → "084265" [ENTER] → [1] → [ENTER] ◆

<Language>: 1 0=KO 1=EN 2=JP 3=SP 4=CN

Default setting: '1' (English)

Voice output languages are as follow, '0': Korean, '1': English, '2': Japanese, '3': Spanish and '4': Chinese.

'0'~'2': LCD characters correspond to the assigned language.
'3'~'4': LCD characters are English.

After the setting is completely done, press [ENTER] to move to the upper menu.

3.8.2. Function key settings

◆ [Fn] → [6] → '084265' [ENTER] → [2] ◆

<Key On/Off> 1=F1:O 2=F2:O 3=F3:O 4=F4:O 5=Ent:O 6=FP:O

Default setting: all 'O'

This is to enable or disable the function keys. [O] means enabling the function key and [X] means disabling the function key. Whenever the number conformed to a function key in this setting is pressed, this setting is changed between O and X.

In this setting, 1 conforms to [F1], 2 conforms to [F2], 3 is for [F3], 4 is for [F4], 5 is for [ENTER], and 6 is for the fingerprint sensor's auto sensing. For example, if an administrator presses [1] one time in this setting and [F1] key is disabled - [X], a user can not enter into start mode by pressing [F1] key button as [F1] key is disabled.

In addition, if only [F1] or [F2] is set to 'O', the terminal can be used just for start mode or for leave mode all the time.

After the setting is completely done, press [ENTER] to move to the upper menu.

3.8.3. Card reader settings

◆ [Fn] → [6] → '084265' [ENTER] → [3] ◆

Card Reader:0 0=Non 1=RF 2=SC 3=Wiegand 4=SC1 5=Ext

Default setting: '0'

This is to set the card reader mounted in a terminal. Refer to the followings for correct setting:

- '0': No card reader
- '1': Low-frequency RF Card reader mounted
- '2': High-frequency smart card reader
- '3': Wiegand card reader like HID card module
- '4': Other smart RF reader
- '5': External card reader

If a card reader is mounted into a terminal and the above setting is correctly done, when [F1]~[F4] or [ENTER] is pressed, the authentication mode is changed and 1:1 fingerprint authentication is ready for operation - in this case, 1:N fingerprint authentication is not performed except for auto sensing setting.

After the setting is completely done, press [ENTER] to move to the upper menu.

3.8.4. Fingerprint sensor settings

3.8.4.1. 1:1 verification level settings

◆ [Fn] → [6] → '084265' [ENTER] → [4] ◆

<1:1 Level> (1-9): 4

Default setting: '4'

This is to set 1:1 matching security level for a terminal between the fingerprint captured from fingerprint input window and the relevant fingerprint stored in a terminal. The higher 1:1 matching level means the higher security. But possibility of authentication failure is getting higher as higher matching rate is required.

For an example of 1:1 authentication with ID input, if inputted ID number is '1234', there is authentication process between the fingerprint captured from fingerprint input window and the fingerprint associated with ID '1234' in a terminal.

For your information, if a user's 1:1 authentication level is set to '0' – refer to 3.3.1.1. "1. FP" registration, 1:1 matching process for the user is performed according to the 1:1 authentication level (1:1 level of a terminal) assigned through "3.8.4.1. 1:1 authentication level for a terminal". If a user's 1:1

authentication level is set to other levels except for '0', 1:1 matching process for the user is performed according to his own 1:1 level.

Press [ENTER] to move to the next setting.

3.8.4.2. 1:N identification level settings

◆ [Fn] → [6] → "084265" [ENTER] → [4] → [ENTER] ◆

<1:N Level> (3-9): 5

Default setting: '5'

This is to set 1:N authentication security level between the fingerprint captured from fingerprint input window and all the fingerprints in a terminal which are allowed for 1:N authentication.

For your information, 1:N authentication level is not set for respective user but only for a terminal.

Press [ENTER] to move to the next setting.

3.8.4.3. Intelligent-Capture settings

◆ [Fn] → [6] → '084265' [ENTER] → [4] → [ENTER] → [ENTER] ◆

<I-Capture> (N=0/Y=1): 1

Default setting: '1'

This adjusts the sensor settings automatically to enhance good fingerprint detection capability by reducing bad influences from humid fingers and/or residual fingerprints which are left on a sensor window due to sweat and/or contaminants on fingertip.

- If it is set to '0', fingerprint capturing time gets shorter but its authentication rate for dry or wet finger becomes lower.
- If it is set to '1', fingerprint capturing time becomes longer than that of above '0' setting but its authentication rate gets higher. Therefore, '1' setting is recommended.

After the setting is completely done, press [ENTER] to move to the upper menu.

3.8.5. Wiegand output settings

◆ [Fn] → [6] → "084265" [ENTER] → [5] ◆

Wiegand Out: 0 0=None 1=26bit 2=34bit

Default setting: '0'

Its default setting is '0'. If Wiegand output from the local terminal is needed for external access controller with Wiegand input, an administrator can set this setting as '1' or '2'.

- In case of '1' setting, "site code [1 byte] and user ID [2 bytes]" are transmitted through Wiegand output port. User ID should be set as less than 4 digits.
- In case of [2] setting, "site code [1 byte] and user ID [3 bytes]" are transmitted through Wiegand output port. User ID should be set as less than 7 digits.

※ This setting is not related to external Wiegand reader.
※ In cases of '1' or '2' settings, the below-mentioned site code should be set.

<Site Code> (0-255): 000

Default setting: '000'

An administrator can assign the site code of from 0 to 255 which is transmitted together with a user ID.

After this setting is completely done, press [ENTER] to move to the upper menu.

3.8.6. Terminal initialization

3.8.6.1. Configuration settings initialization

In the main menu, press [6] to select "6. Device" and then press [6] to select "6. Initialize" and the following screen appears:

1. Init Config 2. Delete Log 3. Init Terminal

Press [1] for configuration settings initialization.

◆ [Fn] → [6] → "084265" [ENTER] → [6] → [1] ◆

<Init Config> [Y=1 / N=2]:

To initialize configuration settings, press [1]. If not, press [2].

All the configuration settings except for Mac (physical) address are initialized;

users' information and authentication records are not deleted.

※ If this configuration settings initialization is done, the language for voice output and display characters is changed to English. If you need to set as other language, refer to the followings; "6. Set Device"→ "1. System Config" → <Language>.

After this configuration settings initialization is successfully done, it moves to the upper menu together with a "ppiririck" buzzer sound.

3.8.6.2. Authentication record initialization

◆ [Fn] → [6] → "084265" [ENTER] → [6] → [2] ◆

<Delete All Log> [Y=1 / N=2]:

To initialize the log data, press [1]. If not, press [2].

All the log data related to authentication are deleted; configuration settings and users' information are not deleted.
After this initialization is successfully done, it moves to the upper menu together with a "ppiririck" buzzer sound.

3.8.6.3. Factory default initialization

◆ [Fn] → [6] → "084265" [ENTER] → [6] → [3] ◆

<Init Terminal> [Y=1 / N=2]:

To initialize everything to factory default, press [1]. If not, press [2].

Except for the Mac (physical) address stored in the terminal, all the configuration settings, users' information and authentication records (log data) are deleted, which becomes same as factory default.

※ If this factory default initialization is done, the language for voice output and display characters is changed to English. If you need to set as other language, refer to the followings; "6. Set Device"→ "1. System Config" → <Language>.

After this initialization is successfully done, the terminal is rebooted with a "ppiririck" buzzer sound.

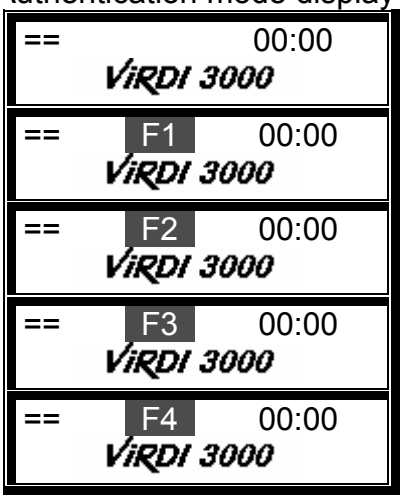
4. How to use the terminal

4.1. Access control

- Menu "3.Option" → "1.Application" → [0] Access control settings

4.1.1. Authentication mode

- Authentication mode display screen



Normal mode; authentication with [ENTER]

F1 mode; authentication with [F1]

F2 mode; authentication with [F2]

F3 mode; authentication with [F3]

F4 mode; authentication with [F4]

※ In access control application, authentication process mainly happens in normal mode by pressing 'Enter' button or using auto sensing without pressing any keys. For more detailed operation in access control application, an administrator can specify F1, F2, F3 and F4 modes at his/her discretion as F1, F2, F3 and F4 modes are not specified as a respectively fixed mode by manufacturer – UNION COMMUNITY.

- Fingerprint authentication
  Fingerprint authentication in the corresponding mode by pressing a relevant function key; 'Enter', F1, F2, F3 and F4.
  Fingerprint authentication through auto sensing without pressing any keys. This authentication is performed in the current mode displayed in the screen.

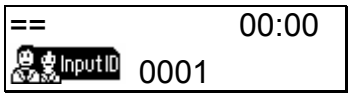
- Password authentication
  After inputting the user ID and changing the authentication mode by pressing the corresponding function key, input the password for authentication.

- Card authentication after the following settings are done: menu → "6.Device" settings → "3.Card reader" → <Card Reader> is set to '1' or over
  Pressing the function key changes just authentication mode. For card authentication, press the corresponding function key and then place the card close to the terminal.

4.1.2. [1:1] fingerprint authentication

▶ When auto sensing is running, input '0001' if the user ID is '0001' and then place your finger close to the fingerprint sensor. The light on the fingerprint input window turns on to detect the fingerprint and the authentication result is displayed on the LCD window.

▶ If the user ID is '0001', input '0001' and press the function key. The light on the fingerprint input window turns on together with voice information. When a fingerprint is inputted, the authentication result is displayed on the LCD window.



If the user ID is '0001', input '1' or '0001' and press the function key.

▼

Place your finger close to the input window when the light on the fingerprint input window turns on together with the voice message "Please enter your fingerprint". Do not remove your finger until you hear a "ppig" buzzer sound.

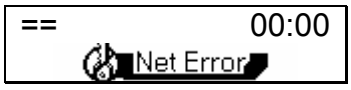
▼

If authentication is successfully done, a success message is displayed on the LCD together with a voice message "You are authorized". The door LED turns on and door relay runs.
The default screen appears after 1~2 seconds. The door LED turns off and door relay is back again after the door open setting time has elapsed.

※ Error message: The following error message appears together with a voice message "Please try again".

In case of authentication failure

Non-registered user ID



During authentication request to the authentication server, network trouble occurred or network line was disconnected.

4.1.3. [1:N] fingerprint authentication

This authentication is allowed only for users who are registered as 1:N authentication setting.

▶ If a user places his/her finger close to the fingerprint sensor when auto sensing is running, the light on the fingerprint input window turns on to detect the fingerprint and the authentication result is displayed on the LCD window.

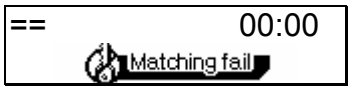
▶ In a main screen, press the function key. The light on the fingerprint input window turns on together with voice information. When a fingerprint is inputted, the authentication result is displayed on the LCD window.

In a main screen, press the function key.

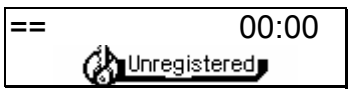
Place your finger close to the input window when the light on the fingerprint input window turns on together with the voice message "Please enter your fingerprint". Do not remove your finger until you hear a "ppig" buzzer sound.

If authentication is successfully done, a success message is displayed on the LCD together with a voice message "You are authorized". The door LED turns on and door relay runs.
The default screen appears after 1~2 seconds. The door LED turns off and door relay is back again after the door open setting time has elapsed.

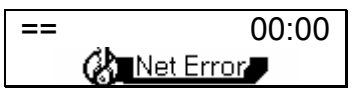
※ Error message: An error message appears together with the voice message "Please try again".



In case of authentication failure



If the connection method is SN – refer to 3.4.2. Connection [NS / SN / NO] mode settings - and there is no user to whom 1:N authentication is allowed in the terminal

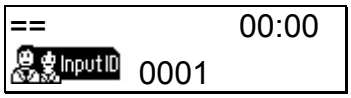


During authentication request to the authentication server, network trouble occurred or network line was disconnected.

▶ In case of a user who is registered as [fingerprint & password], correct password input is required after successful fingerprint authentication.

4.1.4. Password authentication

▶ If the user ID is '0001', input '0001' and press the function key. The terminal waits for the user password to be inputted after a "ppiriririck" buzzer sound. Input the relevant password and press [ENTER]. The authentication result appears on the LCD.



If the user ID is '0001', input '0001' and press the function key.

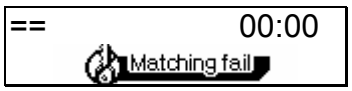
▼

The terminal waits for the user password to be inputted after a "ppiriririck" buzzer sound. Input the relevant password and press [ENTER]. For security reason, the password is displayed as '*' on the LCD screen, not actual numbers.

▼

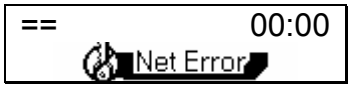
If authentication is successfully done, a success message is displayed on the LCD together with a voice message "You are authorized". The door LED turns on and door relay runs.
The default screen appears after 1~2 seconds. The door LED turns off and door relay is back again after the door open setting time has elapsed.

※ Error message: The following error message appears together with a voice message "Please try again".



In case of authentication failure

Non-registered user ID



During authentication request to the authentication server, network trouble occurred or network line was disconnected.

4.1.5. Card authentication

▶ In case of a user who is registered as [RF], [RF|FP] or [RF|PW], place the card close to the terminal in main screen. After a "ppig" buzzer sound, the authentication result appears on the LCD.

Place your card close to the terminal. It makes a "ppig" buzzer sound.

▼

If authentication is successfully done, a success message is displayed on the LCD together with a voice message "You are authorized". The door LED turns on and door relay runs.
The default screen appears after 1~2 seconds. The door LED turns off and door relay is back again after the door open setting time has elapsed.

※ Error message: The following error message appears together with a voice message "Please try again".

Non-registered card

During authentication request to the authentication server, network trouble occurred or network line was disconnected.

▶ In case of a user who is registered as [RF&FP] or [ID&FP | RF&FP], place the card close to the terminal in main screen. After a "ppig" buzzer sound, the following fingerprint authentication screen appears:

When the light on the fingerprint input window turns on together with the voice message "Please enter your fingerprint", enter your fingerprint and hold it there until you hear a "ppig" buzzer sound.

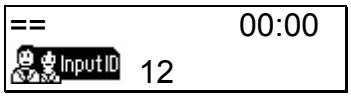
▶ In case of a user who is registered as [RF&PW] or [ID&PW | RF&PW], place the card close to the terminal in main screen. After a "ppig" buzzer sound, the following fingerprint authentication screen appears:

After a "ppiriririck" buzzer sound, the terminal waits for the user password to be inputted. Enter password and press [ENTER].

4.1.6. User ID group authentication

User ID group authentication is performed just among users grouped with same first digit and/or above of user ID – at least one digit. This authentication can conveniently be used if there are too many users and the matching time for 1:N authentication takes too long. In the menu, set as below: 3. Option settings → 2. Authentication method settings → <1:N authentication>=1 → <ID group authentication >=1.

For your information, refer to the followings on how to use this authentication in more details,
If the relevant ID for a user is 1234, enter only 12 for this authentication. This matching is performed just among users having IDs of from 1200 to 1299 , starting with 12. If the ID is '0012', enter '0012' or '00' for authentication.



If the user ID is '1234', enter '1', '12', or '123', and then press the function key.

▼

When the light on the fingerprint input window turns on together with the voice message "Please enter your fingerprint", enter your fingerprint and hold it there until you hear a "ppig" buzzer sound.

▼

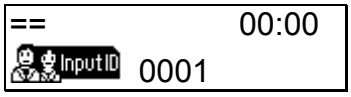
If authentication is successfully done, a success message is displayed on the LCD together with a voice message "You are authorized". The door LED turns on and door relay runs.
The default screen appears after 1~2 seconds. The door LED turns off and door relay is back again after the door open setting time has elapsed.

4.1.7. Multiple fingerprint authentication

For a door where higher security is required, multiple fingerprints captured from more than two persons are assigned to a single ID for access to the specific door. The door opens only when all the registered fingerprints are successfully authenticated. In the menu, set as below: 3. Option setting → 2. Authentication method settings → <1:N authentication >=0 → < multiple fingerprint authentication >=1.

For example, if the ID "0001" is registered with three different fingerprints, all three fingerprints must be authenticated for access after ID input. A single authentication failure in mid course results in overall failure and the whole authentication process should be restarted. This iterative process continues until all three fingerprints are authenticated.

▶ If the user ID is '0001', enter '1' or '0001' and press the function key. The light on the fingerprint input window turns on together with the voice message "Please enter your fingerprint." (during auto sensing, fingerprint input alone is sufficient). When a fingerprint is entered, the authentication result will be displayed on the LCD window.



If the user ID is '0001', input '0001' and press the function key.

When the light on the fingerprint input window turns on together with the voice message "Please enter your fingerprint", place your finger and hold it there until you hear a "ppig" buzzer sound.

If authentication is successfully done, a "ppiririck" buzzer sounds and the light on the fingerprint input window turns on together with the voice message "Please enter your fingerprint". This iterative process continues until all inputted fingerprints have been authenticated.

If authentication is successfully done, a success message is displayed on the LCD together with a voice message "You are authorized". The door LED turns on and door relay runs.
The default screen appears after 1~2 seconds. The door LED turns off and door relay is back again after the door open setting time has elapsed.

※ Error message is same as that of [1:1] authentication.

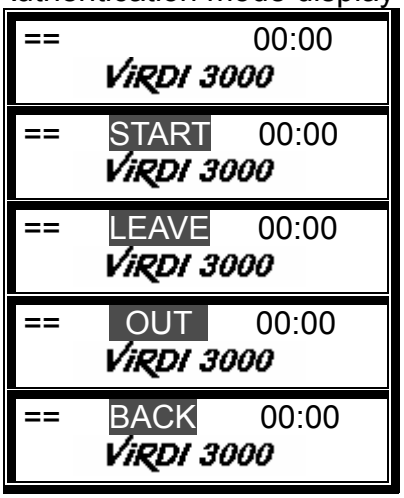
4.2. Time & Attendance control

- Menu "3.Option" → "1.Application" → [1] T&A settings

- If start and leave time for employees are fixed, set <start time>, <leave time> and <normal time> to reduce user input errors.

4.2.1. Authentication mode

- Authentication mode display screen



Normal mode; authentication with [ENTER]

Start mode; authentication with [F1]

Leave mode; authentication with [F2]

Outside work mode; authentication with [F3]

Return mode; authentication with [F4]

- Fingerprint authentication
  Press the function key which is related to specific T & A mode.
  If the function key is not used and authentication process is done in auto sensing, the current mode on the screen is working for authentication.

- Password authentication
  After inputting the user ID and changing the authentication mode by pressing the corresponding function key, input the password for authentication.

- Card authentication after the following settings are done: menu ("6.Device" settings ("3.Card reader" (<Card Reader> is set to [1] or over.
  Pressing the function key changes just authentication mode. For card authentication, press the corresponding function key and then place the card close to the terminal.

- After authentication is done, working mode returns to the mode – start, leave or normal - previously set as time frames but if no mode is set for the specific time period, the previous authentication mode is maintained.

4.2.2. [1:1] fingerprint authentication

- Same as 4.1.2.

4.2.3. [1:N] fingerprint authentication
- Same as 4.1.3.

4.2.4. Password authentication
- Same as 4.1.4.

4.2.5. Card authentication
- Same as 4.1.5.

4.2.6. User ID group authentication
- Same as 4.1.6.

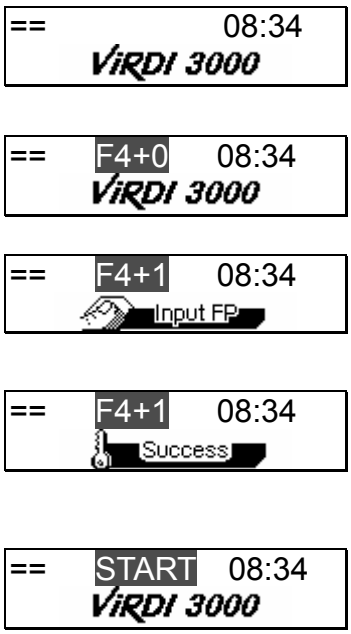
4.2.7. Expansion of working mode by multi-key function

- If more than 5 working modes - start, leave, outside work (out), return (back) and normal - are required, it can be expanded up to 41 modes.

- After setting Menu → 3.Option → 1.Application → [1] T&A, set more than one key to [O] in <Multi Fn-key> setting. The keys set to [X] are not applied in this multi-key function.

- As a mode is defined as a function key plus a number key, press a number key after pressing the function key for authentication. In the server program, authentication mode is displayed as a function key plus a number key like "F3+1".

- For example, when [F4] is set to [O] and <start time> is set to "07:00~09:30", if a fingerprint user tries for authentication in "F4+1"mode,



In main screen, press [F4].

The mode is changed to "F4+0".
Press [1].

When the mode is changed to "F4+1", enter the fingerprint.

When authentication is successfully done, a success message appears.

The current time is 08:34, so it returns to the start mode.

4.3. Meal control

- Menu → "3. Option" → "1.Application" → [2] Meal settings

- If the terminal is set for meal control, as the terminal is in "lock setting!'' status during other time frames except for the meal times previously set, at least more than one time frame as meal time should be set for meal control usage.

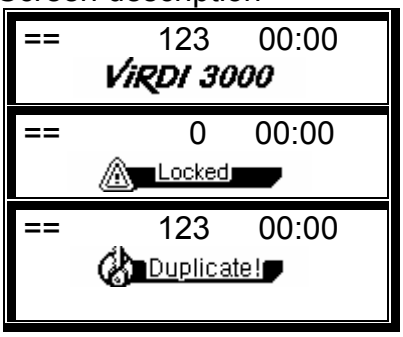
- Basically, a single authentication is allowed for each meal per user but double authentication is also possible by using [ENTER]. Refer to 3.5.1.3. [2]: Meal Control.

- If an administrator wants to prevent double authentication at any time, set as below: Menu → "6.Device settings" → "2.Set Fn-key" settings (Ent=[X] at <Key On/Off>. After this setting is done, double authentication by using [ENTER] is not available.

4.3.1. Meal classification

- In meal control, the function key is just operation key for authentication and there is just meal classification with a meal time frame - there is no mode classification. The number shown in the LCD screen means the number of authentication for a specific meal time period.

- Screen description



Total number of successful authentication is displayed.

Not in meal time period

In case that a user tries double authentication during the same meal time period

- Fingerprint authentication
  Press the function key for authentication.
  When auto sensing is running, a user can place only a finger for authentication without pressing any function key.

- Password authentication
  Enter the user ID, press the function key, and enter the password for authentication

- Card authentication after the following settings are done: menu → "6.Device" settings → "3.Card reader" → <Card Reader> is set to [1] or over.

4.3.2. [1:1] fingerprint authentication
- Same as 4.1.2., but [ENTER] cannot be used as a function key

4.3.3. [1:N] fingerprint authentication
- Same as 4.1.3., but [ENTER] cannot be used as a function key

4.3.4. Password authentication
- Same as 4.1.4., but [ENTER] cannot be used as a function key

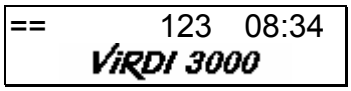
4.3.5. Card authentication
- Same as 4.1.5., but [ENTER] cannot be used as a function key

4.3.6. User ID group authentication
- Same as 4.1.6., but [ENTER] cannot be used as a function key

4.3.7. Double authentication

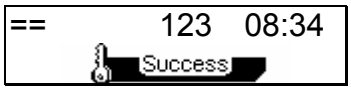
- Set as below: Menu → "6.Device" → "2.Set Fn-key" settings → Ent=[O] at <Key On/Off>. The default setting is [O], so there is no need to change it. However, if it does not work, check this setting again.

- Fingerprint user double authentication



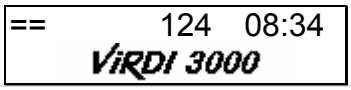
While pressing [ENTER] in the main screen, place your finger.

▼



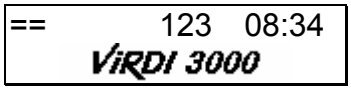
If authentication is successfully done, a success message is displayed.

▼



When it returns to the main screen, the number of meals increases.

- Card user double authentication

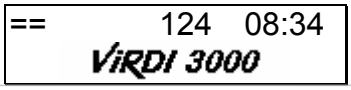


While pressing [ENTER] in the main screen, place a card.

▼

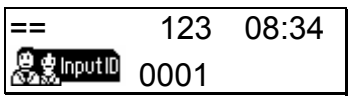
If authentication is successfully done, a success message is displayed.

▼



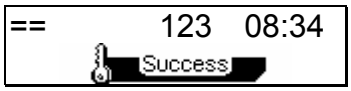
When it returns to the main screen, the number of meals increases.

- Password user double authentication

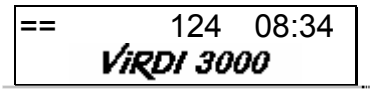


After inputting the user ID in the main screen, press a function key among [F1], [F2], [F3] and [F4] while pressing [ENTER].

With a "ppiriririck" buzzer sound, it waits for the user password to be input. Press [ENTER] after inputting the password.



If authentication is successfully done, a success message is displayed.



When it returns to the main screen, the number of meals increases.